DEPARTMENT OF THE AIR FORCE

AIA RECURRING PERIODICAL 31-1

1st Quarter 2001

Security

THE SHIELD

NOTICE: This publication is available digitally on the AIA website: http://pdc.aia.af.mil/pubs.

OPR: HQ AIA/SOCD (MSgt Guy Woodbury)

Certified by: HQ AIA/SOC (Mr. Robert Eddy)
Pages: 11
Distribution: F

FOREWORD This recurring publication is published quarterly to assist security managers administer unit security training and education programs. It supports the Air Intelligence Agency (AIA) Security Training, Education, and Motivation (STEM) Program governed by AIA Supplement 1 to AFI 31-401, *Managing The Information Security Program*. The contents are for information and training purposes only. Articles presented herein do not represent a change of policy or requirements unless officially incorporated into Air Force or Agency instructions.

We solicit your suggestions for articles or other ideas for publication. We are very interested in "cross-feeding" improved methods, effective procedures, quality enhancements, or other publications and training aids in this publication. Please forward any articles or suggested topics to the Information Security Division, Disclosure Branch, HQ AIA/SOCD, 102 Hall Blvd, Suite 257, San Antonio TX 78243-7026 or e-mail: guy.woodbury@lackland.af.mil.

1. INFORMATION SECURITY:

1.1. MESSAGES TO THE FIELD by MSgt Steve Kramer, HQ AIA/SOCD:

The following messages are from the past quarter and contain policy or guidance from HQ AIA/SO and others. They are intended for use throughout the Agency and supported element security offices; however, some apply only to the Wings, Groups, and Centers. If your organizations is not in receipt of, or on distribution for a below message, forward your inquiry to Mrs. Darleen Benware at DSN 969-2888 or darleen.benware@lackland.af.mil.

1.1.1. JGUBY MESSAGES: Used to disseminate security information to AIA units.

Message Number	Date	Subject
JGUBY 00-16	031100Z Nov 00	FY 01 NRO Special Security Officer (NRO SSO) Course Schedule and Registration

JGUBY 00-17	081439Z Nov 00	Foreign Ownership, Control or Influence (FOCI)
JGUBY 00-18	151407Z Nov 00	AIA Antiterrorism Handbook’s Homepage Posting
JGUBY (Unnumbered)	142224Z Nov 00	DSSCS Address JGUBY Recapitulation
JGUBY 00-19	052151Z Dec 00	AIA Supplement 1 to AFI 31-101 Electronic Publications Posting
JGUBY 00-20	201837Z Dec 00	Posting Copies of JGUBY Messages on AIA’s Products and Services Page on Intelink
JGUBY 00-21	201840Z Dec 00	EPSQ Receipt System – Extension
JGUBY 00-22	291930Z Dec 00	USAF SCI Security Management Course Slides
JGUBY 01-01	161208Z Jan 01	AIA Supp 1/AFM 14-304, The Security, Use, and Dissemination of Sensitive Compartmented Information
JGUBY 01-02	181450Z Jan 01	New Access Procedures for Pentagon
JGUBY 01-03	241438Z Jan 01	ACC/AIA Integration – MAJCOM SSO Oversight
JGUBY 01-04	301758Z Jan 01	Clarification to AIAVA 31-102 (Know Your Credentials), Sep 00, and Entry Credential Fabrication
JGUBY 01-05	051529Z Feb 01	Issue and Use of the Revised AIA Form 57, AIS/Media Authorization Pass
JGUBY 01-06	051829Z Feb 01	Revised AIA Form 31, Nov 00 (EF-V1) Electronic Publications Posting
JGUBY 01-07	081343Z Feb 01	New Periodic Reinvestigation (PR) Reporting Procedures

1.1.2. NOSIZ MESSAGES: Used to disseminate security training information.

Message Number	Date	Subject
NOSIZ 00-11	071607Z Nov 00	USAF SCI Security Management Course Info
NOSIZ (Unnumbered)	142224Z Nov 00	DSSCS Address Group NOSIZ Recapitulation
NOSIZ 00-13	112031Z Dec 00	USAF SCI Security Management Course Info
NOSIZ 00-14	271757Z Dec 00	DIA SCI Security Officials Course FY 01 Schedule
NOSIZ 01-01	032040Z Jan 01	Physical Security Seminar (DCID 1/21) Class Announcement Message

NOSIZ 01-02	221928Z Jan 01	Cancellation of 13-15 Feb 01 USAF SCI Security Management Course
NOSIZ 01-03	082131Z Feb 01	USAF SCI Security Management Course Info

1.1.3. ROXAD MESSAGES: Used to disseminate updates and clarification of policy to the field.

Message Number	Date	Subject
ROXAD 00-05 (AIA-ROXAD-05-00)	121630Z Dec 00	Classified in Open Source Advisory
ROXAD (Unnumbered)	142224Z Nov 00	DSSCS Address Group (DAG) ROXAD
ROXAD 00-06 (AIA-ROXAD-06-00)	131956Z Dec 00	Classified in Public Media/Open Source

1.1.4. AIG 8551: Used to disseminate information to AIA Security Forces.

Message Number	Date	Subject
AIG 8551 00-19	151448Z Nov 00	AIA Security Manager of the Year Award Program
AIG 8551 00-20	061401Z Dec 00	Information Security-Management Information System (MIS) Data Report
AIG 8551 00-21	201558Z Dec 00	Security Office Digest, Fourth Quarter 2000
AIG 8551 01-01	081939Z Feb 01	2000 AIA Security Forces (SF) Individual Awards Program

1.2. DERIVATIVE CLASSIFICATION by MSgt Guy Woodbury, HQ AIA/SOCD

The vast majority of us in the Air Force who produce classified documents are doing what is called derivative classification. What is derivative classification?

Derivative classification is the process of extracting, paraphrasing, restating, or generating information that was taken from a classified document or using the guidance of a classification guide. It is not just the act of photocopying a classified document. An original classification authority must classify new projects or ideas. Who has the authority and responsibility to use derivative classification?

Within the Department of Defense (DoD), all cleared personnel who generate or create material that should be derivatively classified are responsible for ensuring that the derivative classification is accomplished in accordance with DoD 5200.1-R, *Information Security Program*. Personnel doing derivative classification require no specific delegation of authority. If you approve or sign a derivatively classified document you are responsible for the quality of the derivative classification. What policy must be used by personnel performing derivative classification?

There are five rules to use when you derivatively classify a document. They are:

Table 1. Five Rules to Classify a Document.

RULE		
1	OBSERVE AND RESPECT	Observe and respect the classification determinations made by original classification authorities.
2	APPLY MARKINGS	Apply markings or other means of identification to the derivatively classified material.
3	USE ONLY AUTHORIZED SOURCES	Use only authorized sources of instructions about the classification of the information in question. Authorized sources of instructions about classification are security classification guides, other forms of classification guidance, and markings on material from which the information is extracted. The use of only memory or general rules about the classification of broad classes of information is prohibited.
4	USE CAUTION	Use caution when paraphrasing or restating information extracted from a classified source document to determine whether the classification may have been changed in the process.
5	TAKE APPROPRIATE AND REASONABLE STEPS	Take appropriate and reasonable steps to resolve doubts or apparent conflicts about the classification, level of classification, and duration of classification of information. These steps may include consulting a security classification guide or referral to the organization responsible for the original classification. In cases of apparent conflict between a security classification guide and a classified source document about a discrete item of information, the instructions in the security classification guide shall take precedence.

2. PERSONNEL SECURITY:

2.1. CONTRACTOR ATTENDANCE DURING CLASSIFIED MEETINGS by Lenny Martin, HQ AIA/SOPS

You have been selected as the Office of Primary Responsibility (OPR) for a classified conference in the not too distant future. Originally, the plan called for attendance to be by government employees only. However, it has since been decided that some contractors are going to attend. Your Commander wants to know if there are any additional requirements that have to be met in order for this to happen. What’s your answer?

Contractors are *only* allowed access to classified information based upon a “need-to-know” and what’s stated in their contract – nothing more. When there is a classified contractual relationship between the parties involved, classified information may be disclosed without further approval. If not, classified information may *not* be disclosed without approval from the Administrative Assistant to the Secretary of the Air Force (SAF/AA).

To obtain approval a written request is sent to SAF/AA at least *six months* before the conference. The following publications will help you and your Security Manager put together the request:

Table 2. Reference Publications For Classified Conferences.

Publication	Title	Comments
DOD 5200.1-R	*Information Security Program*	Paragraph 6-307 discusses the development of security requirements for classified conferences
DOD 5220.22-M	*National Industrial Security Program Operating Manual*	Paragraph 6-109 identifies when classified may be disclosed to contractors
DOD 5220.22-R	*Industrial Security Program*	Paragraph 1-400 identifies when classified may be disclosed to contractors Paragraph 1-404 identifies locations where classified conferences may *not* be held Paragraph 1-405 identifies the content of conference security procedures
AFI 31-401	*Information Security Program Management*	Paragraph 5.15. Establishes the requirement for a security plan
AFI 61-205	*Sponsoring or Co-Sponsoring, Conducting, and Presenting DOD Related Scientific Papers at Unclassified and Classified Conferences, Symposia, and other Similar Meetings*	Establishes procedures for sponsoring and co-sponsoring classified meetings

2.1.1. So? Do you have an answer for your Commander – are there any additional security requirements to allow contractors to attend? Dependent on whether you have a contractual relationship with them -- You bet there are!

2.2. KNOW THE RULES...WORDS OF WISDOM CONCERNING THAT PART-TIME JOB by SMSgt Danny Shine, HQ AIA/SOP

NOTES:

Portions quoted from article written and presented by Capt. Jesse Arnstein/305th Air Mobility Wing Legal Office.

Honey, sweetheart, the kids need new shoes, and the car needs new tires but we don't have the money in our budget. Do something!!!

Some Air Force members moonlight at other jobs to either make ends meet, pay off bills, or just have extra spending money on hand. Some tend bars, toss pizzas, cut hair, stock shelves, and more.

Air Force people who are thinking about starting an extra job should remember their obligations to the Air Force. Off-duty employment rules are punitive, and violators are subject to disciplinary action.

Military members are required to receive approval from their supervisor and commander via an AF Form 3902, **Application and Approval for Off-Duty Employment,** before beginning off-duty employment. This form can be found on the Air Force Publications Web site at http://afpubs.hq.af.mil. Normally supervisors approve requests, but there are certain types of activities that should not be approved, such as:

Jobs that create a conflict of interest

Jobs that detract from readiness

Jobs involving dangerous activity

Jobs that bring discredit upon the armed forces

For instance, a request to work as a bull rider in a rodeo may not be approved because of the danger involved, and a request to be a go-go dancer would probably be disapproved because it could bring discredit upon the armed forces. A request to work 40 hours per week at another job would likely be disapproved because of the time demand.

These restrictions also apply if military people are engaged in outside employment that does not pay a salary. For instance, approval from your supervisor and commander is needed before volunteering at a local fire department, even if there is no compensation attached.

There are more complex rules for certain medical people, which are detailed in AFI 44-102, *Community Health Management*. There are also rules and reporting requirements that apply to those that may be indoctrinated into Sensitive Compartmented Information (SCI), which are detailed in DoD 5105.21-M-1, *Sensitive Compartmented Information Administrative Security Manual*.

Finally, if the additional employer asks a military member to sign a contract, you should review the document carefully before signing. Sometimes these contracts contain a "covenant not to compete" clause.

This provision might prohibit you from taking a subsequent job in the same vicinity and field as your current job. If so, this may hamper future job prospects. People should read over any contract very carefully and fully understand the commitment they are asked to make. Understanding “conflict of interest” is key to deciding whether you should or should not take that second job.

2.3. NEW ENTRANCE PROCEDURES AT THE PENTAGON—DON’T LEAVE YOUR HOME BASE WITHOUT A VISIT CERTIFICATION by SMSgt Danny Shine, HQ AIA/SOP

There have been significant changes in Pentagon entrance security procedures affecting all visitors. Active and reserve duty military members may gain entrance to the Pentagon by displaying their active duty ID card and a second form of identification while in uniform. However, when out of uniform, active and reserve duty military members must be pre-announced by memorandum along with presenting two forms of ID.

For all others, a memorandum with the subject line of visitor certification must be sent to the Pentagon Pass Office. It must be sent at least three days prior to the visit. The Visitor Certification may be mailed to: Pass Office, Washington Headquarters Service, 1155 Defense Pentagon, Washington DC

20301-1155 or faxed to (703) 697-9085. If the visit is of short notice, last minute accommodations can be worked by calling the Pass Office at (703) 695-5923 or DSN 225-5923.

For Sensitive Compartmented Information (SCI) indoctrinated personnel, this visit memorandum is in addition to forwarding SCI clearances to the Special Security Office. If you plan to visit without forwarding your SCI clearance, you must ensure the visitor certification is forwarded. All security managers should be aware of the new requirement and adjust their procedures accordingly. See your security manager for assistance.

The visitor certification will include:

Full name, SSN, location and date of birth, background investigation date, dates of the visit, POC telephone number of the office being visited, and POC of the visitor's agency.

NOTE:

DO NOT include clearance level, i.e. TS/S/SCI

In addition to the visitor certification, when you arrive at any Pentagon entrance, you must show two forms of identification. Accepted forms of identification are:

Accepted Forms of Identification.

Driver's license or ID card issued by a state or possession of the United States, which contains a photograph or information such as name, date of birth, gender, height, eye color, and address.

ID card issued by federal, state, or local government agency or entity provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address.

School ID card with a photograph.

Voter Registration card.

US Military ID card or draft record.

Military family member ID card.

US Coast Guard Merchant Marine card.

Native American Tribal document.

Driver's license issued by a Canadian government authority.

To avoid any entrance delays while visiting the Pentagon, implement the above-mentioned visitor certification notices immediately...don't leave home without it.

2.4. NEW PUBLICATION by Ardith Meyers, HQ AIA/SOPP

AIA Supplement 1 to AFM 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information,* was published on 8 Dec 00. It is available for download from the SIPRNet AIA worldwide website under Products and Services or the JWICS website at:

http://www.aia.ic.gov/common/product/publications/standardpubs

The supplement is unclassified; however, it is not available on the NIPRNet due to the handling instructions (For Official Use Only) associated with the AFMAN. (See AFI 33-129, *Transmission of Information via the Internet*.) If you have never accessed these sites before, you may need to call upon your AIS or computer work-group manager to download the initial publication for you.

Thanks to those of you who responded with comments and suggestions for inclusion in this supplement. We made every effort to incorporate applicable items into this publication; however, we found some of the suggestions applied to the basic manual and were, therefore, not included. (These items will be forwarded to AF/XOIIS for consideration in the next version of the AFMAN.)

Some of the items detailed in this supplement are:

How to use the Sentinel Key system to administer SCI accesses

Reestablishing nine-digit SCI access management numbers

Reporting procedures for SIF and for-cause actions

Emergency destruction priorities

DAGs used to publish SCI security advisories

How to forward AIA Form 79, *SCI Access Certification*, on-line.

Direct any questions concerning this supplement to Mrs Ardith Myers, 969-4559/4541.

3. PHYSICAL SECURITY

3.1. BUT ISN'T TEMPEST A DEAD PROGRAM? by MSgt Timothy Taylor, HQ AIA/SOXX

During my first session as a briefer for the USAF's SCI Security Management course, I mentioned TEMPEST and one of the attendees asked, "Isn't TEMPEST dead?" Having worked TEMPEST issues in the late 80's and early 90's, I've often had the same thought over the past few years. While recently attending the TEMPEST Fundamentals course, I learned that this seems to be the thought within the Air Force today. What I've discovered is that while the targets and threats have been updated and the publications revised, the program still exists.

What the Air Force once referred to as TEMPEST has been incorporated into what is now called Emission Security, or EMSEC for short. AFI 33-203, *Emission Security*, defines EMSEC as "the protection resulting from all measures taken to deny unauthorized persons information that might be derived from intercepts and the interception and analysis of compromising emanations from crypto-equipment, information systems, and telecommunications systems." It defines TEMPEST as "an unclassified term referring to technical investigations for compromising emanations from electronically operated processing equipment; these investigations are conducted in support of emission security." In 1992, AFSSI 7007 defined TEMPEST as "a short name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment." As you can see the definition has been updated slightly, but the program still warrants attention.

Is there still a threat to our systems and equipment? Yes! One of the most likely TEMPEST targets today could be your computer monitor. It has been identified that video display units emit unique radio-frequency waves that can be isolated and captured with a directional antenna focused on a particular computer or room. Those signals can then be amplified with fairly inexpensive equipment and reconstructed to show precisely what was displayed on the targeted monitor. These signals can travel for long distances much the same as the signals emitted for your local radio station.

What can be done to help prevent or limit these compromising emanations? The answer today is Emission Security Assessment. If you process any type of classified information, contact your local

Information Protection of EMSEC office. They can provide you with guidance for implementing any required countermeasures. After implementation, they will perform an Emission Security Assessment to validate the countermeasure application.

For more information concerning the Emission Security program, requirements, or process refer to AFI 33-203.

4. FORCE PROTECTION

4.1. FORCE PROTECTION PLAN DEVELOPMENT by MSgt Donald Shea, HQ AIA/SOXX

Force protection is a security program designed to protect resources: people, facilities, and equipment. It is accomplished through the planned and integrated application of other programs such as antiterrorism and counter-terrorism, physical security, personal protective services, and intelligence programs. The purpose of this article is to develop an understanding of the roles of all responsible parties.

Responsibility for force protection flows from the President to the Office of the Secretary of Defense (OSD) to the Civilian Services Secretaries of the Army, Navy, and Air Force, to the Joint Chiefs of Staff, the combatant commands, the Inspector General of DOD, and the Defense Agencies.

The responsibility for force protection is inherent at all levels of the Air Force. It begins with the Air Staff and follows a chain of command through major commands (MAJCOMs), installation commanders, and to the various installation-level organizations associated with security and facility planning and design. Installation commanders have the ultimate responsibility to plan and implement force protection strategies at the local level. Force Protection Working Groups at the Air Staff, unified and specified commands, MAJCOM, and installation levels promote awareness and provide guidance to the development of a Force Protection Program.

Individual and organizational force protection roles and responsibilities must be practiced and publicized in order to have an effective Force Protection Program. Once personnel and organizations recognize their new roles and responsibilities for integrating force protection, the daily practices they employ for mission accomplishment will eventually incorporate force protection (or will develop a force protection orientation).

The following summarizes the roles and responsibilities of organizations having an active role in force protection.

Air Staff: The directorate of The Civil Engineer, DCS/Installations & Logistics (HQ USAF/ILE) provides direction and advocates funding support for force protection. The Force Protection Division, under the Director of Security forces (HQ USAF/SF), provides force protection resource advocacy, policy, and guidance to the field. The division is composed of Security Forces, Intelligence, and Office of Special Investigations resources. These resources, combined with the other Air Staff organizations of Operations, Civil Engineer, Surgeon General, Logistics, Personnel, and Services, make up the Force Protection Working Group.

Security Forces Center: Collocated with the Air Force Security Forces Academy at Lackland AFB, this Direct Reporting Unit (DRU) of Air Staff was designated as a “center of excellence” for force protection. The AF Security Forces Staff, 820th Security Forces Group, and The Force Protection Battle Lab comprise The Security Forces Center. The Security Forces Center is composed of representatives from the Office of Special Investigations, Intelligence, Communications, Security Forces, and Civil Engineer, which includes Explosive Ordnance Disposal.

The 820th Security Forces Group provides a highly trained cohesive unit that can be employed as the initial security force element at deployed locations to establish force protection infrastructure and ensure maximum protection to deployed forces. It also makes force protection recommendations to Installation Commanders utilizing AF OSI threat assessments. Collocated with the Security Forces Group, an Office of Special Investigations Antiterrorism Specialty Teams (AST) provides specialized investigative force protection services including vulnerability surveys of installation, facilities, buildings, and travel routes; counter-surveillance of potential terrorist target; and responses to specific terrorist incidents.

Air Force Civil Engineer Support Agency (AFCESA): AFCESA, a Field Operating Agency (FOA) of the Civil Engineer, provides engineering expertise and related information on force protection. The Wright Lab Detachment, collocated with AFCESA, conducts research on explosive testing and analysis of building design and materials to minimize damage as a result of an explosion. Examples of Wright Labs force protection initiatives include planning tools, blast and fragment barriers, structural retrofits, and glass protection. Wright Labs also provides direct assistance to the Air Force operational community in the areas of terrorist weapon effects, installation and facility assessments, and design and analysis of physical protection measures.

Air Force Center for Environmental Excellence (AFCEE): As a FOA and Air Staff service agency, AFCEE executes projects and issues planning and design guidance. AFCEE is the “keeper” of the Force Protection Guide and will be responsible for updating it with new force protection information.

Unified and Specified Commands: Provide policy and guidance to component commanders regarding threat and force protection measures.

Office of Special Investigations (OSI): In addition to promoting force protection awareness, OSI conducts vulnerability assessments and surveys. OSI also collects intelligence data on terrorist threats through an established intelligence source network, counter-surveillance of potential terrorist groups, and response to specific terrorist incidents.

Major Commands (MAJCOMs): Planners, designers, and engineers at the MAJCOM level provide guidance and oversee the implementation of force protection standards at the installation level.

Installation Commander: Ultimate responsibility for implementing force protection measures at the installation level rests with the Installation Commander. The Installation Commander chairs the Installation Security Council (ISC) and/or the Resource Protection Executive Committee (RPEC) and initiates the installation’s response to identify threats through the ISC/RPEC.

Installation Security Council (ISC)/Resource Protection Executive Committee (RPEC): An ISC (at installations that support priority resources) manages force protection activities including a vulnerability assessment to critical assets to identified threats and preparation of the Installation Security Plan (ISP). This installation-level organization may be combined with the RPEC. The committee is chaired by the Installation Commander and is composed of, but not limited to, representatives from Office of Special Investigations, Security Forces, Civil Engineers, Fire, Safety, Communications, and Transportation. In addition to validating and reviewing programming and project design, the ISC should monitor installation facility planning, design, and construction activities to ensure that they comply with established force protection strategies. The ISC/RPEC publishes Installation Security

Plans (ISP) which can be combined with the Installation Resource Protection Plan (IRPP) and with other related operation plans (OPLAN) into one ISP. (See SFI 31-209, The Air Force Resource Protection Program).

Base Civil Engineer (BCE) and Installation Community Planner: The Base Civil Engineer, supported by the installation's community planner and the ISC/IRPEC, ensures that facility force protection measures are included in the Installation Security Plan/Installation Resource Protection Plan. The BCE is also responsible for the integration of force protection measures into the installation's general plan, area development plans, and facility designs.

Programmers: Programmers are responsible for integrating force protection measures during project scooping. They ensure that force protection measures are included in the special requirement section of DD Form 1391 in accordance with AFI 32-1021, *Planning and Programming of Facility Construction Projects*.

Facility Designers: Facility designers include installation architects, planners, landscape architects, engineers, project managers, and contracted consulting architect-engineers (A-Es). They are responsible for integrating force protection measures during the facility and site design process.

Force protection refers to measures designed to protect personnel, facilities, and equipment that support national defense missions. These measures are aimed at minimizing loss of life and other critical assets. The Air Force objective as prescribed by AFI 31-210, *The Air Force Antiterrorism (AT) Program*, "is to reduce the vulnerability of personnel and facilities to terrorism while balancing defensive measures with mission requirements and available resources." Future articles to appear in "The Shield" will explain how to consciously integrate antiterrorism measures into facility planning, design, and construction efforts.

JIMMY R. JONES
Chief of Security